MICHIGAN INTELLIGENCE OPERATIONS CENTER

Privacy Policy

---

1. STATEMENT OF PURPOSE

The goal of establishing and maintaining the Michigan Intelligence Operations Center (MIOC) is to further the following purposes:

1.1. Increase public safety and improve national security;

1.2. Minimize the threat and risk of injury to specific individuals;

1.3. Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

1.4. Minimize the threat and risk of damage to real or personal property;

1.5. Protect individual privacy, civil rights, civil liberties, and other protected interests;

1.6. Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

1.7. Minimize reluctance of individuals or groups to use or cooperate with the justice system;

1.8. Support the role of the justice system in society;

1.9. Promote governmental legitimacy and accountability;

1.10. Not unduly burden the ongoing business of the justice system; and

1.11. Make the most effective use of public resources allocated to justice agencies.

2. COMPLIANCE WITH LAWS REGARDING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

2.1 The MIOC, all participating agency personnel, personnel providing information technology services to the agency, private contractors, and users will comply with all applicable laws, to which they are legally bound, protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

2.2 The contents of this privacy policy provide internal guidance to participating MIOC personnel. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any

administrative, civil, or criminal matter by any prospective or actual witnesses or parties. See United States v. Caceres, 440 U.S. 741 (1979).

3 DEFINITIONS

3.1 Agency - agency refers to the Michigan Intelligence Operations Center (MIOC).

3.2 Information - information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

3.3 Law - as used in this policy, *law* includes any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal officials or agencies.

3.4 Public – public includes any of the following:

3.4.1 Any person and any for-profit or nonprofit entity, organization, or association;

3.4.2 Any governmental entity for which there is no existing specific law authorizing access to the agency's information;

3.4.3 Media organizations; and

3.4.4 Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

3.4.5 Employees of the agency;

3.4.6 People or entities, private or governmental, who assist the agency in the operation of the justice information system; and

3.4.7 Public agencies whose authority to access information gathered and retained by the agency is specified in law.

3.5 Purge – purge refers to the deletion or destruction of information and data.

4 SEEKING AND RETAINING INFORMATION

4.1 Information sought and retained

4.1.1 This agency will seek or retain only information:

4.1.1.1 Relevant to the investigation and prosecution of suspected criminal (including a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an

intelligence service or network of a foreign power or by its agent) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; the prevention of crime; or in the administration of criminal justice.

4.1.1.2 Collected by criminal justice agencies on specific individuals, consisting of official identifiable descriptions and notations of arrests, detentions, warrants, complaints, indictments, information, or other formal criminal charges and any disposition relating to these charges, including acquittal, sentencing, pre- or post conviction supervision, correctional supervision, and release.

4.1.1.3 Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent) conduct or activity.

4.1.2 This agency will not seek or retain information about an individual or organization solely on the basis of activities protected by the first amendment to the Constitution of the United States and parallel provisions in Article I of the Constitution of the State of Michigan.

4.1.3 This agency will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any individual or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:

4.1.3.1 Relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal (including a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent) activity; and

4.1.3.2 Needed by the agency:

4.1.3.2.1 To identify an individual,

4.1.3.2.2 In order for the agency to operate effectively, or

4.1.3.2.3 To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

4.1.4 The agency shall keep a record of the source of all information retained by the agency.

4.2 Methods of Seeking or Receiving Information

4.2.1 Information gathering and investigative techniques used by this agency will comply with all applicable state and federal laws.

4.2.2 Information gathering and investigative techniques used by this agency will be no more intrusive or broad scale than is necessary in the particular circumstance to gather information it is authorized to seek or retain pursuant to Subsection 4.1.

4.3 Classification of information regarding validity and reliability

4.3.1 At the time of retention in the system, the information will be categorized regarding its:

4.3.1.1 Content validity;
4.3.1.2 Nature of the source; and
4.3.1.3 Source reliability.

4.3.2 The categorization of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

4.4 Classification of information regarding limitations on access and disclosure

4.4.1 At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

4.4.1.1 Protect confidential sources and police undercover techniques and methods;
4.4.1.2 Not interfere with or compromise pending criminal investigations;
4.4.1.3 Protect an individual's right of privacy and civil rights; and
4.4.1.4 Provide legally required protection based on the status of an individual as a victim or witness.
4.4.1.5 Provide and ensure protection against unauthorized or prohibited disclosure.

4.4.2 The classification of existing information will be reevaluated whenever:

4.4.2.1 New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
4.4.2.2 There is a change in the use of the information affecting access or disclosure limitations.

4.4.3 The access classifications will be used to control:

4.4.3.1 What information a class of users can have access to;
4.4.3.2 What information a class of users can add, change, delete or print; and
4.4.3.3 To whom the information can be disclosed and under what circumstances.

5 INFORMATION QUALITY

5.1 The agency will make every reasonable effort to ensure that information sought or retained is:

5.1.1 Derived from dependable and trustworthy sources of information;
5.1.2 Accurate;
5.1.3 Current; and
5.1.4 Complete, including the relevant context in which it was sought or received and other related information.

5.2 The agency will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

5.3 The agency will make every reasonable effort to ensure that information will be deleted from the system when the agency learns that:

5.3.1 The information is erroneous, misleading, obsolete, or otherwise unreliable;

5.3.2 The source of the information did not have authority to gather the information or to provide the information to the agency

5.4 The agency will advise recipient agencies when information previously provided to them is deleted or changed pursuant to Subsection 5.3.

6 COLLATION AND ANALYSIS OF INFORMATION

6.1 Collation and analysis

6.1.1 Information sought or received by the agency or from other sources will only be analyzed:

6.1.1.1 By qualified individuals;

6.1.1.2 To provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals, and organizations suspected of having engaged in or engaging in criminal, including terrorist, activities generally; and

6.1.1.3 To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.

6.1.2 Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates Subsection 4.1.2.

6.2 Merging of information from different sources

6.2.1 Information about an individual or organization from two or more sources will not be merged.

7 SHARING AND DISCLOSURE OF INFORMATION

7.1 Sharing information within the agency and with other justice system partners

7.1.1 Access to information retained by this agency will only be provided to persons within the agency or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with the law and procedures applicable to the agency for whom the person is working.

7.1.2 The person, who received, reviewed, or added information to the system may be authorized to view the information he or she provided regardless of the type of access associated with the information or the contributor's access authority.

7.1.3 An audit trail will be kept of access by or dissemination of information to such persons.

7.2 Sharing information with those responsible for public protection, safety, or public health

7.2.1 Information retained by this agency may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

7.2.2 Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

7.2.3 The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

7.2.4 An audit trail will be kept of the access by or dissemination of information to such persons.

7.3 Sharing Information for Specific Purposes

7.3.1 Information gathered and retained by this agency may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

7.3.2 The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

7.3.3 An audit trail will be kept of the requests for access and of what information is disseminated to such persons.

7.4 Disclosing information to the public

7.4.1 The agency will ensure that information gathered and retained by this agency may be disclosed to a member of the public only if the information complies with the Michigan Freedom of Information Act and, where applicable, 5 U.S.C. 552a.

7.4.2 The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

7.4.3 An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

7.5 Disclosing Information to the Individual About Whom Information Has Been Gathered

7.5.1 Upon satisfactory verification of his or her identity and subject to the conditions specified in Subsection 7.5.2., an individual is entitled to know the existence of and to review the information about him or herself that has been gathered and retained by the agency. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The agency's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.

7.5.2 The existence, content, and source of the information will not be made available to an individual when:

7.5.2.1 Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;

7.5.2.2 Disclosure would endanger the health or safety of an individual, organization, or community;

7.5.2.3 The information is in a criminal intelligence system.

7.5.2.4 The information is classified National Security Information (NSI) or Grand Jury information as defined by Rule 6 of the Federal Rules of Criminal Procedure.

7.5.2.5 Disclosure is otherwise prohibited by law.

7.5.3 If an individual has objections to the accuracy or completeness of the information retained about him or herself, the agency will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if a request for correction is denied. The individual will also be informed of the procedure for appeal when the agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

7.5.4 A record will be kept of all requests and of what information is disclosed to an individual.

8 INFORMATION RETENTION AND DESTRUCTION

8.1 Review of information regarding retention

8.1.1 The review of information for purging will be an ongoing process as set forth in the agency Review-and-Purge policy and in accordance with 28 CFR Part 23 and all applicable state laws.

8.1.2 When information has no further value or meets the criteria for removal under applicable law, it will be purged.

8.2 Purging of information

8.2.1 The agency will delete or destroy information according to 28 CFR Part 23 and all applicable state laws.

8.2.2 Permission to purge information or records will be obtained from the entering member or source, MIOC Command, or automatically in accordance with the Review-and-Purge policy.

8.2.3 Destruction of records will be conducted without notice in accordance with the agency Review-and-Purge policy.

8.2.4 Only an administrative record of the purge will be maintained. No record of the names of individuals, organizations, etc., that are purged will be maintained by the agency.

9 ACCOUNTABILITY AND ENFORCEMENT

9.1 Information system transparency

9.1.1 The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request.

9.1.2 The agency will designate a person responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system and will provide contact information to the public.

9.2 Accountability for activities

9.2.1 The agency will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with the Global Justice Information Sharing Initiative (Global) recommendations on information sharing.

9.2.2 The agency will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as provided in 28 CFR Part 23 and all applicable state laws.

9.2.3 Through the adoption of information system security practices, logging of access requests and responses, and detection of unauthorized attempts to add, change, delete, or access information, audit practices, and other enforcement mechanisms, the agency will be able to evaluate the compliance of users and the system itself with the provisions of this policy and applicable law.

9.2.4 The agency will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy and in the event of a conflict with the individual's participating agency policies, seek agency authorization prior to any deviation from this policy.

9.2.5 The agency will periodically conduct audits and inspections of the information contained in the MIOC. The audits will be conducted randomly by a designated representative of the agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

9.2.6 The agency will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

9.2.7 The agency will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any

measures necessary to determine the scope of the release of information and to reasonably restore the integrity of the information system. Notice need not be given if doing so meets the criteria specified in Subsection 7.5.2.

9.3 Enforcement

9.3.1 If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the agency may, at the discretion of MIOC Command:

9.3.1.1 Suspend or discontinue access to information by the user;

9.3.1.2 Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;

9.3.1.3 Apply other sanctions or administrative actions as provided in agency personnel policies;

9.3.1.4 Request the participating agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or

9.3.1.5 Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy as stated in Section 1.

9.3.1.6 Members of the Michigan State Police Troopers Association (MSPTA) are not subject to provisions 9.3.1.2 through 9.3.1.5, of this policy, as their conduct is governed by department Official Orders and the Collective Bargaining Agreement between the State of Michigan and the MSPTA.

10 TRAINING

10.1 The agency will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

10.1.1 Its personnel;
10.1.2 Personnel providing information technology services to the agency;
10.1.3 Staff in other public agencies or private contractors providing services to the agency; and
10.1.4 Users who are not employed by the agency or a contractor.

10.2 The training program will cover:

10.2.1 Purposes of the privacy, civil rights, and civil liberties protection policy;
10.2.2 Substance and intent of the provisions of the policy relating to collecting, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;
10.2.3 The impact of improper activities associated with information accessible within or through the agency; and
10.2.4 The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

10.2.5 Members of the Michigan State Police Troopers Association (MSPTA) are not subject to provisions 10.2.3 and 10.2.4, of this policy, as their conduct is governed by department Official Orders and the Collective Bargaining Agreement between the State of Michigan and the MSPTA.